

Claims

What is claimed is:

1 1. A method for determining a level of trust in an authenticated identification, comprising:

3 performing at least one authentication to obtain an authentication result,

4 each authentication having a score, each result indicating

5 whether the corresponding authentication is successful; and

6 combining the scores for the successful authentications to determine a

7 level of trust.

1 2. The method of claim 1, wherein performing at least one authentication
2 comprises authenticating a purported identification.

1 3. The method of claim 1, wherein performing at least one authentication
2 comprises authenticating a purported identification of one selected from the
3 group consisting of a person, a document, and an item.

1 4. The method of claim 1, further comprising:

2 responsive to the determined level of trust exceeding a predetermined
3 threshold, allowing access to a resource.

1 5. The method of claim 1, further comprising:

2 responsive to the determined level of trust exceeding a predetermined
3 threshold, selecting a role for a user.

1 6. The method of claim 1, further comprising:

2 responsive to the determined level of trust exceeding a predetermined
3 threshold, offering a user a role for selection.

1 7. The method of claim 1, further comprising:

2 responsive to the determined level of trust not exceeding a predetermined
3 threshold, denying access to a resource.

1 8. The method of claim 1, further comprising:

2 responsive to the determined level of trust exceeding a first predeter-
3 mined threshold, allowing a first level of access to a resource;
4 and
5 responsive to the determined level of trust exceeding a second predeter-
6 mined threshold, allowing a second level of access to a resource.

1 9. The method of claim 8, wherein each level of access corresponds to an
2 allowed action with respect to the resource.

1 10. The method of claim 8, wherein the first level of access comprises
2 reading the resource and the second level of access comprises modifying the re-
3 source.

1 11. The method of claim 4, 7, 8, 9, or 10, wherein the resource comprises a
2 document.

1 12. The method of claim 1, further comprising:
2 receiving a request for an action, the action being associated with a prede-
3 termined minimum level of trust;
4 responsive to the determined level of trust exceeding the predetermined
5 minimum level of trust, allowing the requested action to pro-
6 ceed; and
7 responsive to the determined level of trust not exceeding the predeter-
8 mined minimum level of trust, denying the requested action.

1 13. The method of claim 1, further comprising:
2 presenting a list of allowable actions having minimum trust levels not ex-
3 ceeding the determined level of trust.

1 14. The method of claim 13, further comprising:
2 receiving input specifying one of the presented actions; and
3 initiating the specified action.

1 15. The method of claim 1, wherein combining the scores comprises de-
2 termining a sum of the scores for the successful authentications.

1 16. The method of claim 1, wherein each authentication is performed ac-
2 cording to an authentication method, and wherein the score for each authentica-
3 tion is associated with the corresponding authentication method.

1 17. The method of claim 16, where each authentication method is selected
2 from the group consisting of:
3 password authentication;
4 secret question authentication;
5 smartcard authentication;
6 processor identification;
7 biometric identification; and
8 location identification.

1 18. The method of claim 1, wherein performing at least one authentication
2 comprises determining a characteristic of a network connection.

1 19. The method of claim 18, wherein the determined characteristic of the
2 network connection comprises a physical location of a computer connected via
3 the network.

1 20. The method of claim 18, wherein the determined characteristic of the
2 network connection comprises a degree of security associated with the network
3 connection.

1 21. The method of claim 18, wherein the determined characteristic of the
2 network connection comprises a previous authentication.

1 22. The method of claim 1, wherein each score indicates a relative degree
2 of reliability of the corresponding authentication.

1 23. The method of claim 1, further comprising:
2 responsive to the determined level of trust, determining whether to allow
3 or deny each of a plurality of requested actions during a user
4 session.

1 24. A system for determining a level of trust in an authenticated identifi-
2 cation, comprising:

3 an authenticator, for performing at least one authentication to obtain an
4 authentication result, each authentication having a score, each
5 result indicating whether the corresponding authentication is
6 successful; and
7 a score combiner, coupled to the authenticator, for combining the scores
8 for the successful authentications to determine a level of trust.

1 25. The system of claim 24, wherein performing at least one authentica-
2 tion comprises authenticating a purported identification.

1 26. The system of claim 24, wherein the authenticator authenticates a
2 purported identification of one selected from the group consisting of a person, a
3 document, and an item.

1 27. The system of claim 24, wherein the authenticator, responsive to the
2 determined level of trust exceeding a predetermined threshold, allows access to a
3 resource.

1 28. The system of claim 24, wherein the authenticator, responsive to the
2 determined level of trust exceeding a predetermined threshold, selects a role for
3 a user.

1 29. The system of claim 24, wherein the authenticator, responsive to the
2 determined level of trust exceeding a predetermined threshold, offers a user a
3 role for selection.

1 30. The system of claim 24, wherein the authenticator, responsive to the
2 determined level of trust not exceeding a predetermined threshold, denies access
3 to a resource.

1 31. The system of claim 24, wherein the authenticator, responsive to the
2 determined level of trust exceeding a first predetermined threshold, allows a first
3 level of access to a resource, and, responsive to the determined level of trust ex-

4 ceeding a second predetermined threshold, allows a second level of access to a
5 resource.

1 32. The system of claim 31, wherein each level of access corresponds to an
2 allowed action with respect to the resource.

1 33. The system of claim 31, wherein the first level of access comprises
2 reading the resource and the second level of access comprises modifying the re-
3 source.

1 34. The system of claim 27, 30, 31, 32, or 33, wherein the resource com-
2 prises a document.

1 35. The system of claim 24, further comprising:
2 an action input device, couple to the authenticator, for receiving a request
3 for an action, the action being associated with a predetermined
4 minimum level of trust;

5 wherein the authenticator, responsive to the determined level of trust ex-
6 ceeding the predetermined minimum level of trust, allows the requested action
7 to proceed, and, responsive to the determined level of trust not exceeding the
8 predetermined minimum level of trust, denies the requested action

1 36. The system of claim 24, further comprising:

2 an output device, coupled to the authenticator, for presenting a list of al-
3 lowable actions having minimum trust levels not exceeding the
4 determined level of trust.

1 37. The system of claim 36, further comprising:
2 an input device, coupled to the output device, for receiving input specify-
3 ing one of the presented actions; and
4 a transaction manager, coupled to the input device, for initiating the speci-
5 fied action.

1 38. The system of claim 24, wherein the score combiner determines a sum

2 of the scores for the successful authentications.

1 39. The system of claim 24, wherein each authentication is performed ac-

2 cording to an authentication method, and wherein the score for each authentica-
3 tion is associated with the corresponding authentication method.

1 40. The system of claim 39, where each authentication method is selected

2 from the group consisting of:

3 password authentication;

4 secret question authentication;

5 smartcard authentication;

6 processor identification;

7 biometric identification; and

8 location identification.

1 41. The system of claim 24, wherein the authenticator performs at least
2 one authentication by determining a characteristic of a network connection.

1 42. The system of claim 41, wherein the determined characteristic of the
2 network connection comprises a physical location of a computer connected via
3 the network.

1 43. The system of claim 41, wherein the determined characteristic of the
2 network connection comprises a degree of security associated with the network
3 connection.

1 44. The system of claim 41, wherein the determined characteristic of the
2 network connection comprises a previous authentication.

1 45. The system of claim 24, wherein each score indicates a relative degree
2 of reliability of the corresponding authentication.

1 46. The system of claim 24, wherein the authenticator, responsive to the
2 determined level of trust, determines whether to allow or deny each of a plural-
3 ity of requested actions during a user session.

1 47. A computer-readable medium for determining a level of trust in an
2 authenticated identification, comprising:
3 computer-readable code adapted to perform at least one authentication to
4 obtain an authentication result, each authentication having a
5 score, each result indicating whether the corresponding authen-
6 tication is successful; and
7 computer-readable code adapted to combine the scores for the successful
8 authentications to determine a level of trust.

1 48. The computer-readable medium of claim 47, wherein the computer-
2 readable code adapted to perform at least one authentication comprises com-
3 puter-readable code adapted to authenticate a purported identification.

1 49. The computer-readable medium of claim 47, wherein the computer-
2 readable code adapted to perform at least one authentication comprises com-
3 puter-readable code adapted to authenticate a purported identification of one se-
4 lected from the group consisting of a person, a document, and an item.

1 50. The computer-readable medium of claim 47, further comprising:
2 computer-readable code adapted to, responsive to the determined level of
3 trust exceeding a predetermined threshold, allow access to a re-
4 source.

1 51. The computer-readable medium of claim 47, further comprising:
2 computer-readable code adapted to, responsive to the determined level of
3 trust exceeding a predetermined threshold, select a role for a
4 user.

1 52. The computer-readable medium of claim 47, further comprising:
2 computer-readable code adapted to, responsive to the determined level of
3 trust exceeding a predetermined threshold, offer a user a role
4 for selection.

1 53. The computer-readable medium of claim 47, further comprising:
2 computer-readable code adapted to, responsive to the determined level of
3 trust not exceeding a predetermined threshold, deny access to a
4 resource.

1 54. The computer-readable medium of claim 47, further comprising:
2 computer-readable code adapted to, responsive to the determined level of
3 trust exceeding a first predetermined threshold, allow a first
4 level of access to a resource, and, responsive to the determined
5 level of trust exceeding a second predetermined threshold, al-
6 lowing a second level of access to a resource.

1 55. The computer-readable medium of claim 54, wherein each level of ac-
2 cess corresponds to an allowed action with respect to the resource.

1 56. The computer-readable medium of claim 54, wherein the first level of
2 access comprises reading the resource and the second level of access comprises
3 modifying the resource.

1 57. The computer-readable medium of claim 50, 53, 54, 55, or 56, wherein
2 the resource comprises a document.

1 58. The computer-readable medium of claim 47, further comprising:
2 computer-readable code adapted to receive a request for an action, the ac-
3 tion being associated with a predetermined minimum level of
4 trust;
5 computer-readable code adapted to, responsive to the determined level of
6 trust exceeding the predetermined minimum level of trust, al-
7 low the requested action to proceed, and, responsive to the de-
8 termined level of trust not exceeding the predetermined mini-
9 mum level of trust, deny the requested action.

1 59. The computer-readable medium of claim 47, further comprising:

2 computer-readable code adapted to present a list of allowable actions hav-
3 ing minimum trust levels not exceeding the determined level of
4 trust.

1 60. The computer-readable medium of claim 59, further comprising:
2 computer-readable code adapted to receive input specifying one of the
3 presented actions; and
4 computer-readable code adapted to initiate the specified action.

1 61. The computer-readable medium of claim 47, wherein the computer-
2 readable code adapted to combine the scores comprises computer-readable code
3 adapted to determine a sum of the scores for the successful authentications.

1 62. The computer-readable medium of claim 47, wherein the computer-
2 readable code adapted to perform at least one authentication performs each au-
3 thentication according to an authentication method, and wherein the score for
4 each authentication is associated with the corresponding authentication method.

1 63. The computer-readable medium of claim 62, where each authentica-
2 tion method is selected from the group consisting of:
3 password authentication;
4 secret question authentication;
5 smartcard authentication;

6 processor identification;
7 biometric identification; and
8 location identification.

1 64. The computer-readable medium of claim 47, wherein the computer-
2 readable code adapted to perform at least one authentication comprises com-
3 puter-readable code adapted to determine a characteristic of a network connec-
4 tion.

1 65. The computer-readable medium of claim 64, wherein the determined
2 characteristic of the network connection comprises a physical location of a com-
3 puter connected via the network.

1 66. The computer-readable medium of claim 64, wherein the determined
2 characteristic of the network connection comprises a degree of security associ-
3 ated with the network connection.

1 67. The computer-readable medium of claim 64, wherein the determined
2 characteristic of the network connection comprises a previous authentication.

1 68. The computer-readable medium of claim 47, wherein each score indi-
2 cates a relative degree of reliability of the corresponding authentication.

1 69. The computer-readable medium of claim 47, further comprising:

2 computer-readable code adapted to, responsive to the determined level of
3 trust, determine whether to allow or deny each of a plurality of
4 requested actions during a user session.

1 70. A system for determining a level of trust in an authenticated identifi-
2 cation, comprising:

3 authenticating means, for performing at least one authentication to obtain
4 an authentication result, each authentication having a score,
5 each result indicating whether the corresponding authentication
6 is successful; and
7 score combining means, coupled to the authenticating means, for combin-
8 ing the scores for the successful authentications to determine a
9 level of trust.

1 71. The system of claim 70, wherein the authenticating means, responsive
2 to the determined level of trust exceeding a predetermined threshold, allows ac-
3 cess to a resource.

1 72. The system of claim 70, wherein the authenticating means, responsive
2 to the determined level of trust exceeding a predetermined threshold, selects a
3 role for a user.

1 73. The system of claim 70, wherein the authenticating means, responsive
2 to the determined level of trust exceeding a predetermined threshold, offers a
3 user a role for selection.

1 74. The system of claim 70, wherein the authenticating means, responsive
2 to the determined level of trust not exceeding a predetermined threshold, denies
3 access to a resource.

1 75. The system of claim 70, wherein the authenticating means, responsive
2 to the determined level of trust exceeding a first predetermined threshold, allows
3 a first level of access to a resource, and, responsive to the determined level of
4 trust exceeding a second predetermined threshold, allows a second level of ac-
5 cess to a resource.